JOURNAL OF ALGEBRA **180**, 22–40 (1996)
ARTICLE NO. 0050

Products of Free Groups in the Unit Group of Integral Group Rings*

Eric Jespers†

Department of Mathematics and Statistics, Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1C 5S7

Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro RJ, Brazil

and

Angel del Río§

Departamento de Matemáticas, Universidad de Murcia, 30071 Murcia, Spain

Communicated by Walter Feit

Received December 16, 1994

We classify the nilpotent finite groups G which are such that the unit group $\mathcal{U}(\mathbf{Z}G)$ of the integral group ring $\mathbf{Z}G$ has a subgroup of finite index which is the direct product of noncyclic free groups. It is also shown that nilpotent finite groups having this property can be characterised by means of the Wedderburn decomposition of the rational group algebra $\mathbf{Q}G$. © 1996 Academic Press, Inc.

Let $\mathcal{U}(\mathbf{Z}G)$ denote the unit group of the integral group ring $\mathbf{Z}G$ of a finite group G. There are several results (cf. [12, 13]) showing that $\mathcal{U}(\mathbf{Z}G)$ satisfies some group theoretical property if and only if G is of some

* This work was done while the first and second named authors were staying at the Department of Mathematics of the University of Murcia. They thank the department for its warm hospitality and for the pleasant working conditions.
† Supported in part by NSERC Grant OGP 0036631, Canada, and by the DGICYT, Spain., E-mail address: ejespers@albert.math.mun.ca.
‡ Partially supported by CNPq, Brasil. E-mail address: mad02009@ufrj.bitnet.
§ Partially supported by DGICYT Grant PB90-0300-C02-02. E-mail address: adelrio@fcu.um.es.

0021-8693/96 $18.00

restricted type. In this paper we study the nilpotent finite groups G such that $\mathscr{U}(\mathbf{Z}G)$ has a subgroup of finite index which is the direct product of noncyclic free groups. In the first part we show the surprising result that such groups can be characterised via the structure of the Wedderburn decomposition of the rational group algebra $\mathbf{Q}G$. In the second part we give an exhaustive list of the groups with this property. Finally we show that if a group G is of this type then the trivial units have a normal complement in $\mathscr{U}(\mathbf{Z}G)$ and this normal complement has a subnormal series with noncyclic free factors. Note that in [5] it is shown that there are only two nilpotent (and two non-nilpotent) groups G which are such that $\mathscr{U}(\mathbf{Z}G)$ has a noncyclic free subgroup of finite index.

Throughout paper we use the following notation. By C_n^k we denote the direct product of k copies of the cyclic group with n elements. For convenience, we often consider the group C_2 as a field with two elements and C_2^k as a vector space over C_2. The dihedral group of order $2m$ is denoted by D_{2m} and the quaternion group of order $2m$ is denoted by Q_{2m}. For a subgroup H of a finite group G we denote by $\hat{H}$ the idempotent $(1/|H|)\Sigma_{h \in H} h$. If $g \in G$, then $\hat{g}$ denotes $\langle \hat{g} \rangle$.

Then $n \times n$ matrix ring over a ring R is denoted by $M_n(R)$ and $GL_n(R)$ is its group of invertible matrices. By $\mathbf{H}(R)$ we denote the quaternion ring over R. The center of a ring R (respectively group G) is denoted by $Z(R)$ (respectively $Z(G)$.)

1. GROUPS VERSUS UNIT GROUPS OF INTEGRAL GROUP RINGS

For every subgroup H of G let ω_H: $\mathbf{Z}G \to \mathbf{Z}(G/H)$ be the canonical ring homomorphism and $\Delta(G, H) = \operatorname{Ker}(\omega_H)$. We set $\omega = \omega_G$ and $\Delta(G) = \Delta(G, G)$.

The group of units of a ring R is denoted by $\mathscr{U}(R)$. We several times will use the following fact (see [13, Section 1.4]): if R_1 and R_2 are $\mathbf{Z}$-orders in a finite dimensional $\mathbf{Q}$-algebra, then $R_1 \cap R_2$ is also a $\mathbf{Z}$-order and $[\mathscr{U}(R_1): \mathscr{U}(R_1 \cap R_2)] < \infty$.

For a finite group G, let $M = \sum_e \mathbf{Z}Ge$, where the sum runs through the primitive central idempotents of $\mathbf{Q}G$. Since $\mathbf{Z}G \subseteq M$ are $\mathbf{Z}$-orders in $\mathbf{Q}G$, it follows that H is a subgroup of finite index in $\mathscr{U}(\mathbf{Z}G)$ if and only if H contains a subgroup of finite index in each $\mathscr{U}(\mathbf{Z}Ge)$. Note that again we abuse notation by identifying $\mathscr{U}(\mathbf{Z}Ge)$ with $\mathscr{U}(\mathbf{Z}Ge) + (1 - e)$. Furthermore, for each e write $\mathbf{Q}Ge = M_{n(e)}(D(e))$ where $D(e)$ is a division ring. Let $\mathscr{O}(e)$ be a maximal order in $D(e)$. Then H is a subgroup of finite index in $\mathscr{U}(\mathbf{Z}G)$ if and only if H contains a subgroup of finite index in $GL_{n(e)}(\mathscr{O}(e))$ for all e (also here we identify naturally $GL_{n(e)}(\mathscr{O}(e))$ with

$GL_{n(e)}(\mathcal{O}(e)) + (1 - e))$. By $SL_{n(e)}(\mathcal{O}(e))$ we denote the subgroup of $GL_{n(e)}(\mathcal{O}(e))$ that consists of all elements having reduced norm one.

In this section we prove the following theorem relating the structure of the unit group with the structure of the Wedderburn decomposition.

THEOREM 1. *For any nonabelian nilpotent finite group G the following conditions are equivalent*:

1. *$U(\mathbf{Z}G)$ contains a subgroup of finite index which is isomorphic to a finite direct product of noncyclic free groups.*

2. *for every primitive central idempotent e of $\mathbf{Q}G$, $\mathbf{Q}Ge$ is a commutative field or isomorphic to either the quaternions $\mathbf{H}(\mathbf{Q})$ or to $M_2(\mathbf{Q})$.*

For the sake of shortness we will say that a group G is *admissible* if it satisfies condition 2 of the theorem.

In order to prove the theorem we need some lemmas. In [2] Banieqbal describes all finite subgroups of $GL_2(D)$, where D is a division ring. It follows (see for example [8]) that the only nonabelian nilpotent finite subgroup of $GL_2(\mathbf{Q})$ is D_8, the dihedral group of order 8. In particular, if e is a central idempotent of $\mathbf{Q}G$ such that $\mathbf{Q}Ge \simeq M_2(\mathbf{Q})$, then $Ge \simeq D_8$. However, this can be shown easily when G is a 2-group as follows.

LEMMA 2. *Let G be a 2-group and e a primitive central idempotent of $\mathbf{Q}G$, such that $\mathbf{Q}Ge \simeq M_2(\mathbf{Q})$. Then $Ge \simeq D_8$.*

Proof. By [4, Proposition 23.16] one may assume that $\mathbf{Z}Ge \subseteq M_2(\mathbf{Z})$. The canonical epimorphism $M_2(\mathbf{Z}) \to M_2(\mathbf{Z}_2)$ restricts to a group homomorphism $f: Ge \to GL_2(\mathbf{Z}_2)$. Let

$$K = \left\{ A \in \begin{pmatrix} 1 + 2\mathbf{Z} & 2\mathbf{Z} \\ 2\mathbf{Z} & 1 + 2\mathbf{Z} \end{pmatrix} \middle| \det(A) = 1 \right\}.$$

Since $K/\{I, -I\}$ is a free group [10] it follows that $|K \cap \mathrm{Ker}(f)| \leq 2$ and hence $|\mathrm{Ker}(f)| \leq 4$. Since $GL_2(\mathbf{Z}_2)$ has six elements and Ge is a nonabelian 2-group, we obtain that Ge is either D_8 or Q_8. However, Q_8 is impossible as $\mathbf{Q}Q_8$ does not have $M_2(\mathbf{Q})$ as a simple component. ∎

LEMMA 3. *Let G be a 2-group and e a primitive central idempotent of $\mathbf{Q}G$, such that $\mathbf{Q}Ge \simeq \mathbf{H}(\mathbf{Q})$. Then $Ge \simeq Q_8$.*

Proof. Since Ge is a subgroup of the multiplicative group of a division ring (in particular it is fixed point free), then $Ge \simeq Q_{2^n} = \langle a, b : a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, bab^{-1} = a^{-1} \rangle$ for some $n \geq 3$ [11, Theorem 18.1.iv]. Therefore QGe is isomorphic to a simple component of $\mathbf{Q}Q_{2^n}$. Because $\mathbf{Q}Q_{2^n} \simeq \mathbf{Q}D_{2^{n-1}} \oplus \mathbf{H}(\mathbf{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1}))$ and $\mathbf{Q}D_{2^{n-1}}$ has not any simple component isomorphic to $\mathbf{H}(\mathbf{Q})$ (cf. [13, Lemma 20.4]), the assumption implies that $\mathbf{H}(\mathbf{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1})) \simeq \mathbf{H}(\mathbf{Q})$. Hence $n = 3$ and thus $Ge \simeq Q_8$. ▮

LEMMA 4. *If G is a nilpotent admissible nonabelian finite group then both $Z(G)$ and $G/Z(G)$ have exponent* 2.

Proof. Let $e_1, e_2, \ldots, e_n$ be the complete set of primitive central idempotents of $\mathbf{Q}G$. Any Ge_i can be considered as a multiplicative subgroup of $\mathbf{Q}G$ and the map $f: G \to \prod_{i=1}^n Ge_i$ given by $f(g) = (ge_1, \ldots, ge_n)$ is an injective homomorphism of groups such that $\pi_i \circ f$ is surjective for every i ($\pi_i : \prod_{i=1}^n Ge_i \to Ge_i$ the ith projection). Any Ge_i is either abelian or $\mathbf{Q}Ge_i \simeq M_2(\mathbf{Q})$ or $\mathbf{Q}Ge_i \simeq \mathbf{H}(\mathbf{Q})$. By Lemmas 2 and 3, if Ge_i is nonabelian then it is isomorphic to either Q_8 or D_8. Assume $H = Ge_1 \times \cdots \times Ge_k$ is abelian and $K = Ge_{k+1} \times \cdots \times Ge_n$, where any G_i is not abelian for every $i > k$. Then $f(Z(G)) \subset H \times Z(K)$ and hence f induces an injective homomorphism $f' : G/Z(G) \to K/Z(K) \simeq \prod_{i=k+1}^n Ge_i/Z(Ge_i) \simeq C_2^{2(n-k)}$. Thus $G/Z(G)$ has exponent 2.

Let $g \in Z(G)$. Then $g(1 - \widehat{G'})$ is a periodic central unit of $\mathbf{Q}G(1 - \widehat{G'})$ and because of [3] and the assumptions $\mathbf{Q}G(1 - \widehat{G'}) \simeq M_2(\mathbf{Q})^n \times \mathbf{H}(\mathbf{Q})^m$ for some $m, n \geq 0$. But every periodic central unit of $M_2(\mathbf{Q})$ and $\mathbf{H}(\mathbf{Q})$ has order at most 2. Thus $g^2(1 - \widehat{G'}) = 1 - \widehat{G'}$ and hence $(g^2 - 1)\widehat{G'} = g^2 - 1$. Since G is not abelian, $G' \neq 1$ and comparing coefficients it follows that $g^2 \in G'$. Consequently $g^2 = g^2\widehat{G'} + g^2(1 - \widehat{G'}) = \widehat{G'} + (1 - \widehat{G'}) = 1$. ▮

Proof of Theorem 1. Part (2) implies (1). Let $N_0 = U(\mathbf{Z}G) \cap (1 + \Delta(G)\Delta(G, Z(G)))$. By Lemma 4 and [13, Lemma 30.6], N_0 is a normal complement of the trivial units $\pm G$ in $\mathscr{U}(\mathbf{Z}G)$, in particular N_0 is of finite index in $\mathscr{U}(\mathbf{Z}G)$. Hence it follows from the remarks preceding the theorem that, for any primitive central idempotent e of $\mathbf{Q}G$ which is such that $\mathbf{Q}Ge = M_2(\mathbf{Q})$, the group N_0 contains a subgroup N_e of finite index in $GL_2(\mathbf{Z}) \subseteq \mathbf{Q}Ge$. Note that Lemma 2 yields that $Ge = D_8$. Let $f: \mathbf{Z}G \to \mathbf{Z}(Ge) = \mathbf{Z}D_8$ be the natural epimorphism. It follows that $N_e \simeq f(N_e) \subseteq f(N_0) \subseteq \mathscr{U}(\mathbf{Z}D_8) \cap (1 + \Delta(D_8)\Delta(D_8, Z(D_8))) = X$. Since X is a free group of rank 3 [6] we obtain that N_e is a noncyclic free group.

We now claim that the direct product $F = \prod_e N_e$, where e runs through the primitive central idempotents of $\mathbf{Q}G$ such that $\mathbf{Q}Ge = M_2(\mathbf{Q})$, is of finite index in $\mathscr{U}(\mathbf{Z}G)$. For this is sufficient to show that F contains a subgroup of finite index in the unit group of a maximal order of $\mathbf{Q}Ge$ for any primitive central idempotent e of $\mathbf{Q}G$. Since the unit group of $\mathbf{H}(\mathbf{Z})$ is isomorphic with Q_8 and because $\mathbf{H}(\mathbf{Z})$ is a maximal order in $\mathbf{H}(\mathbf{Q})$ this is clear when $\mathbf{Q}Ge = \mathbf{H}(\mathbf{Q})$. Hence because of the assumption and the construction of F we only have to deal with the remaining case, that is, when $\mathbf{Q}Ge$ is a field. By [3] this field is a simple component of $\mathbf{Q}(G/G')$. Because of Lemma 4, the abelian group G/G' has exponent 2 or 4. Hence it is well known (see for example [13, Proposition 2.8]) that $\mathbf{Q}Ge \simeq \mathbf{Q}(\xi)$, where ξ is a primitive root of unity of order 1, 2, or 4. It is well known that then the torsion free rank of $\mathscr{U}(\mathbf{Z}[\xi])$ is zero and thus $\mathscr{U}(\mathbf{Z}[\xi])$ is finite. So F indeed contains a subgroup of finite index in the unit group of the ring of integers of the field $\mathbf{Q}Ge$.

Part (1) implies (2). Write $\mathbf{Q}G \oplus_3 M_{n(e)}(D(e))$, where the sum runs through all primitive central idempotents of $\mathbf{Q}G$, with each $D(e)$ a division algebra and $\mathscr{O}(e)$ a chosen maximal order in $D(e)$. By the assumption, let $F = \prod_{i=1}^{n} F_i$ be a subgroup of finite index in $\mathscr{U}(\mathbf{Z}G)$, with each F_i a noncyclic free group. Since $F \cap Z(\mathscr{U}(\mathbf{Z}G)) \subseteq Z(F) = \{1\}$ it follows that $Z(\mathscr{U}(\mathbf{Z}G))$ is finite. Consequently, for any primitive central idempotent $e \in \mathbf{Q}G$, the commutative domain $Z(\mathscr{O}(e))$ has finite unit group. Hence the well known Dirichlet's unit theorem yields that $Z(D)$ is either the rationals or a quadratic imaginary extension of the rationals. Since G is nilpotent, it therefore follows from Theorem 5.2 and Theorem 5.3 in [8] that $D(e) = \mathbf{H}(\mathbf{Q})$ provided $n(e) \leq 2$ and $D(e)$ is nonabelian.

For completeness' sake we include a brief proof for the latter statement in the case $n(e) = 1$. From the classification of finite subgroups of division rings by Amitsur [1] it follows that the only possible nilpotent finite subgroups of a division ring are of the type $Q_{2n} \times C_m$, with m odd. Since subgroups of division rings are fixed point free this also follows from Theorem 18.8.iv in [11]. Since $\mathbf{Q}(Q_{2n} \times C_m) \simeq \mathbf{Q}Q_{2n} \otimes \mathbf{Q}C_m$ one obtains from the Wedderburn decomposition of the respective group algebras that the only possible simple component of $\mathbf{Q}(Q_{2n} \times C_m)$ which is a noncommutative division ring is $\mathbf{H}(\mathbf{Q}(\xi_{2^{\alpha-1}} + \xi_{2^{\alpha-1}}^{-1}) \otimes \mathbf{Q}(\xi_\beta))$ for some $\alpha > 2$, β a positive odd integer. For such a ring to be a division ring it is necessary and sufficient that $\alpha = 2$ and that the order of 2 modulo β is odd. However, the condition on the finiteness of the unit group of the central units in the maximal order yields that $\beta = 1$. Hence $D(e) = \mathbf{H}(\mathbf{Q})$. The case $n(e) = 2$ needs more work and is ultimately based on Banieqbal's classification of finite subgroups of 2×2-matrices over division rings [2].

Next we show that if e is a primitive central idempotent with $n(e) \geq 2$ then $SL_{n(e)}(\mathscr{O}(e))$ contains a subgroup of finite index which is the direct product of noncyclic free groups. Since F is of finite index in $\mathscr{U}(\mathbf{Z}G)$ we obtain that

$$\left[\mathscr{U}\left(\oplus_e M_{n(e)}(\mathscr{O}(e))\right) : F\right] < \infty.$$

Hence, for any primitive central idempotent e,

$$H_e = F \cap SL_{n(e)}(\mathscr{O}(e))$$

is of finite index in $SL_{n(e)}(\mathscr{O}(e))$ (the latter, as a subgroup of $GL_{n(e)}(\mathscr{O}(e))$, is identified with $SL_{n(e)}(\mathscr{O}(e)) + (1 - e)$). Note that since $\mathscr{U}(Z(\mathscr{O}(e)))$ is finite, the group H_e is also of finite index in $GL_{n(e)}(\mathcal{O}(e))$. Write

$$T_e = \prod_{f \neq e} H_f,$$

where the product runs through all the primitive central idempotents f different from a given central idempotent e. Clearly $H_e T_e = H_e \times T_e \subseteq F$ is a subgroup of finite index in $\prod_e SL_{n(e)}(\mathcal{O}(e))$, and thus is also of finite index in $\prod_e GL_{n(e)}(\mathcal{O}(e))$ and F.

Now, fix e and assume $n(e) \geq 2$. We claim that for any $1 \leq i \leq n$ either $p_i(H_e) = \{1\}$ or $p_i(T_e) = \{1\}$, where for each $1 \leq i \leq n$, $p_i : F \to F_i$ is the natural epimorphism. For this, first suppose that $p_i(H_e)$ is not cyclic. Then, since $[p_i(H_e), p_i(T_e)] = \{1\}$ and since F_i is noncyclic and free, one obtains that $p_i(T_e) = \{1\}$. (For this one uses that if a and b are non-trivial commuting elements in F_i, then they generate a cyclic group.) Similarly, if $p_i(T_e)$ is not cyclic, then $p_i(H_e) = \{1\}$. On the other hand, it is impossible that both $p_i(H_e)$ and $p_i(T_e)$ are cyclic. Indeed, for otherwise $[p_i(H_e), p_i(T_e)] = 1$ implies that $p_i(H_e \times T_e)$ is a cyclic subgroup of finite index in F_i, a contradiction. So the claim follows. Let $J = \{i | 1 \leq i \leq n, p_i(H_e) \neq \{1\}\}$. Note that J is not empty as $n(e) \geq 2$ and thus $H_e \neq \{1\}$. The previous claim yields that for each $j \in J$, $F_j \cap H_e$ is of finite index in F_j; in particular, $F_j \cap H_e$ is noncyclic. Consequently $\prod_{j \in J}(H_e \cap F_j)$ is a direct product of noncyclic free groups in $SL_{n(e)}(\mathcal{O}(e))$.

Next we show that each $n(e) < 3$. Suppose the contrary, that is, let e be a primitive central idempotent such that $n(e) \geq 3$, and let H be a subgroup of finite index in $SL_{n(e)}(\mathcal{O}(e))$ which is the direct product of noncyclic free groups. Clearly H is noncentral in $SL_{n(e)}(\mathcal{O}(e))$ and H' is normalized by H. It then follows from the congruence subgroup theorems (see for example [13, Theorem 19.30 and Theorem 19.32]) that the commutator group is of finite index in $SL_{n(e)}(\mathcal{O}(e))$. Hence H' is of finite index in H, a contradiction (note that the commutator subgroup of a nontrivial free group is of infinite index). Thus $n(e) < 3$.

To finish the proof it remains to show that if $n(e) = 2$ then $D(e) = \mathbf{Q}$. So suppose that $n(e) = 2$ and $D(e) \neq \mathbf{Q}$. Let $H = \prod_{i=1}^{l} H_i$ be a subgroup of finite index in $SL_{n(e)}(\mathcal{O}(e))$, with each H_i noncyclic and free. Again denote by $p_i : H \to H_i$ the natural epimorphism. Write by αE_{12} the matrix in $M_2(\mathcal{O}(e))$ with all entries zero except the $(1, 2)$ entry which equals α. We know from the above that $\mathcal{U}(\mathcal{O}(e))$ is finite, say of order less than or equal to m, and also there exists $\beta, \gamma \in \mathcal{O}(e)$ such that the additive group generated by these two elements is free abelian of rank two. Note that because H is of finite index, there exists a nonzero integer v such that $x = (1 + \beta E_{12})^v = 1 + v\beta E_{12} \in H$, and similarly $1 + v\gamma E_{12} \in H$. Because $[x, y] = 1$, we have $[p_1(x), p_1(y)] = 1$. Hence either $p_1(x) = 1$, or $p_1(y) =$

1 or $p_1(x)^s = p_1(x)^t$ for some nonzero integers s, t. In the latter case $p_1(x^s y^{-t}) = 1$. So, in any case, there always exists an element of the type $1 \neq z = 1 + \alpha E_{12} \in H$ such that $p_1(z) = 1$. But then $H_1 \subseteq C_{SL_{n(e)}(\mathscr{O}(e))}(z)$. However, this is in contradiction with the following fact which is easily verified (note that we use here that the unit group of $\mathscr{O}(e)$ is finite of order less than or equal to m.) If $0 \neq \alpha \in \mathscr{O}(e)$ and $a, b \in C_{SL_{n(e)}(\mathscr{O}(e))}(1 + \alpha E_{12})$ then $a^m b^m = b^m a^m$. ∎

We now give the structure of the full unit group $\mathscr{U}(\mathbf{Z}G)$ for any nilpotent admissible finite group G.

PROPOSITION 5. *Let G be a nonabelian nilpotent finite group such that $\mathbf{Q}G$ is the direct sum of simple components that are commutative fields or are isomorphic to either $\mathbf{H}(\mathbf{Q})$ or $M_2(\mathbf{Q})$, then $\mathscr{U}(\mathbf{Z}G)$ has a subnormal series*

$$\{1\} = N_n \subset N_{n-1} \subset \cdots \subset N_0 \subset \mathscr{U}(\mathbf{Z}G)$$

such that N_0 is a normal complement of the trivial units, each N_{i-1}/N_i is free noncyclic, and n is the number of simple components of $\mathbf{Q}G$ isomorphic to $M_2(\mathbf{Q})$.

Proof. Let N_0 be as defined in the first part of the proof of Theorem 1 and let $e_1, e_2, \ldots, e_k$ be all the primitive central idempotents e of $\mathbf{Q}G$ such that $\mathbf{Q}Ge \simeq M_2(\mathbf{Q})$. Further, for each $1 \leq i \leq k$, let $f_i : \mathscr{U}(\mathbf{Z}G) \to \mathscr{U}(\mathbf{Z}Ge_i)$ be the natural group homomorphism. We define the following normal series

$$\mathscr{U}(\mathbf{Z}G) \supset N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k \supset N_{k+1} = \{1\}$$

where

$$N_i = N_{i-1} \cap \ker(f_i),$$

for each $1 \leq i \leq k$.

We now claim that $N_0 e = \{e\}$ for every primitive central idempotent $e \notin \{e_1, \ldots, e_k\}$. Indeed, because of Lemma 3, Ge is either abelian or Q_8. Hence [13, Lemma 30.6] implies that $Ge \cap (1 + \Delta(Ge)\Delta(Ge, Z(G)e)) \cap (\pm Ge) = \{e\}$. It now follows easily that $N_0 e = \{e\}$.

Because of the claim we obtain that

$$N_k \subseteq N_0 e_k$$

and

$$N_{i-1}/N_i \simeq N_{i-1} e_i \subseteq N_0 e_i,$$

for each $1 \leq i \leq k$. Again as in the first part of the proof of Theorem 1, $N_0 e_i$ contains a subgroup of finite index in $GL_2(\mathbf{Z})$ and, moreover, the group $N_0 e_i$ is (up to isomorphism) embedded in the free group $\mathscr{U}(\mathbf{Z}D_8) \cap (1 + \Delta(D_8)\Delta(D_8, D_8'))$. Therefore the result follows. ∎

2. GROUPS VERSUS RATIONAL GROUP ALGEBRAS

For every $n \geq 1$ we denote by W_n the group given by the presentation

$$W_n = \langle x_1, x_2, \dots, x_n | x_i^4 = \left[x_i, [x_j, x_k]\right] = \left[x_i, x_j^2\right] = 1,$$
$$i, j, k = 1, 2, \dots, n \rangle.$$

For every $1 \leq i < j \leq n$ we denote $t_{ij} = [x_i, x_j]$. It is not difficult to see that

$$Z(W_n) = \prod_{1 \leq i < j \leq n} \langle t_{ij} \rangle \times \prod_{i=1}^{n} \langle x_i^2 \rangle \simeq C_2^m \qquad \text{with } m = \binom{n+1}{2}$$

and

$$W_n / Z(Q_n) = \prod_{i=1}^{n} \langle x_i Z(W_n) \rangle \simeq C_2^n.$$

The aim of this section is to prove the following theorem.

THEOREM 6. *For a nilpotent finite group G, the following conditions are equivalent*:

1. *For every primitive central idempotent e of $\mathbf{Q}G$, $\mathbf{Q}Ge$ is a commutative field*, $\mathbf{H}(\mathbf{Q})$, *or* $M_2(\mathbf{Q})$.
2. *G is abelian or $G \simeq H \times C_2^k$ for some $k \geq 0$ and H is isomorphic to exactly one of the following groups*
   (a) W_2.
   (b) $W_2 / \langle x_1^2 \rangle$.
   (c) $W_2 / \langle x_1^2 t_{12} \rangle$.
   (d) $W_2 / \langle x_1^2, x_2^2 \rangle \simeq D_8$.
   (e) $W_2 / \langle x_1^2 t_{12}, x_2^2 t_{12} \rangle \simeq Q_8$.
   (f) $G_{2^{2n}}^1 = W_n / \langle t_{ij} | 2 \leq i < j \leq n \rangle \times \langle x_i^2 | 2 \leq i \leq n \rangle$ $(n \geq 3)$.
   (g) $G_{2^{2n}}^2 = W_n / \langle t_{ij} | 2 \leq i < j \leq n \rangle \times \langle x_i^2 t_{1i} | 2 \leq i \leq n \rangle$ $(n \geq 3)$.
   (h) $G_{2^{2n-1}}^1 = W_n / \langle t_{ij} | 2 \leq i < j \leq n \rangle \times \langle x_i^2 | 1 \leq i \leq n \rangle$ $(n \geq 3)$.
   (i) $G_{2^{2n-1}}^2 = W_n / \langle t_{ij} | 2 \leq i < j \leq n \rangle \times \langle x_i^2 t_{1i} | 2 \leq i \leq n \rangle \times \langle x_1^2 \rangle$ $(n \geq 3)$.

(j) $G^3_{2^{2n-1}} = W_n/\langle t_{ij} | 2 \leq i < j \leq n\rangle \times \langle x_i^2 t_{1i} | 2 \leq i \leq n\rangle \times \langle x_1^2 t_{12}\rangle$ ($n \geq 3$).

First we prove two lemmas.

LEMMA 7. *The class of admissible groups is closed under homomorphic images and subgroups.*

Proof. If H is a homomorphic image of G, then $\mathbf{Q}H$ is isomorphic to a homomorphic image of $\mathbf{Q}G$. Therefore, the first statement is trivial.

Let H be a subgroup of a admissible group G and e a primitive central idempotent of $\mathbf{Q}H$. There exists a primitive central idempotent $f \in \mathbf{Q}G$ such that $fe \neq 0$. Then the map $x \mapsto xf$ is a ring homomorphism $\mathbf{Q}He \to \mathbf{Q}Gf$ which is injective because $\mathbf{Q}He$ is simple. Since $\dim_{\mathbf{Q}} \mathbf{Q}Gf \leq 4$ the second statement also follows. ∎

LEMMA 8. *Let G be a nilpotent nonabelian finite group. Then G is admissible if and only if G is isomorphic to a group of the form $H \times C_2^k$ where H is an indecomposable admissible 2-group and $k \geq 0$. In particular, every nonabelian nilpotent admissible group is a 2-group.*

Proof. Assume that G is admissible. Since G is nilpotent, write $G = G_1 \times G_2$ where G_1 is a 2-group and G_2 is a group of odd order. If G_2 is nonabelian, then by Lemma 7, $\mathbf{Q}G_2$ has a simple component isomorphic to either $M_2(\mathbf{Q})$ or $\mathbf{H}(\mathbf{Q})$. Hence $\mathbf{Q}G_2$ has a simple component of dimension 4 over $\mathbf{Q}$. But this yields a contradiction with [4, Theorem 27.11]. Thus G_2 is abelian and hence G_1 is not. Therefore $\mathbf{Q}G_1$ has a direct summand isomorphic to either $\mathbf{H}(\mathbf{Q})$ or $M_2(\mathbf{Q})$. If $G_2 \neq 1$, then $\mathbf{Q}G_2$ has a direct summand isomorphic to $\mathbf{Q}(\xi)$ where ξ is a primitive pth root of unity with $p \neq 2$. Hence $\mathbf{Q}G \simeq \mathbf{Q}G_1 \otimes \mathbf{Q}G_2$ has a simple component isomorphic to either $\mathbf{H}(\mathbf{Q}) \otimes \mathbf{Q}(\xi) \simeq \mathbf{H}(\mathbf{Q}(\xi))$ or $M_2(\mathbf{Q}) \otimes \mathbf{Q}(\xi) \simeq M_2(\mathbf{Q}(\xi))$, a contradiction.

Since G is finite we thus obtain that $G = G_1 \times G_2 \times \cdots \times G_n$, where any G_i is an indecomposable 2-subgroup of G. If there exist $i \neq j$ such that both G_i and G_j are nonabelian, then both $\mathbf{Q}G_i$ and $\mathbf{Q}G_j$ have a simple component isomorphic to either $\mathbf{H}(\mathbf{Q})$ or $M_2(\mathbf{Q})$. Consequently $\mathbf{Q}[G_i \times G_j]$ has a simple component isomorphic to one of the following rings $\mathbf{H}(\mathbf{Q}) \otimes \mathbf{H}(\mathbf{Q}) \simeq M_4(\mathbf{Q})$, $\mathbf{H}(\mathbf{Q}) \otimes M_2(\mathbf{Q}) \simeq M_2(\mathbf{H}(\mathbf{Q}))$, or $M_2(\mathbf{Q}) \otimes M_2(\mathbf{Q}) \simeq M_4(\mathbf{Q})$, again a contradiction. Therefore, $G = H \times K$ where H is indecomposable and K is abelian. A similar argument to the previous one shows that K has exponent at most 2. Hence $G \simeq H \times C_2^k$.

The converse is obvious. ∎

Proof of Theorem 6. (2) ⇒ (1) By Lemma 8 it is enough to show that any of the 10 indecomposable groups in the list is admissible. Since any of these groups is an epimorphic image of some W_n, it is generated by the images of the x_i's. We will abuse notation and will denote the image of x_i (resp. t_{ij}) by x_i (resp. t_{ij}).

(a) Let $G = W_2$. Write $e = \widehat{t_{12}}$ and for every $a = (a_1, a_2) \in C_2^2$ let

$$f_a = \tfrac{1}{4}\left(1 + (-1)^{a_1} x_1^2\right)\left(1 + (-1)^{a_2} x_2^2\right)(1 - e).$$

It is not difficult to see that $\{e\} \cup \{f_a | a \in C_2^2\}$ is a set of orthogonal central idempotents of $\mathbf{Q}G$. Clearly $\mathbf{Q}Ge$ is commutative, $\dim_{\mathbf{Q}} \mathbf{Q}Ge = 16$, $\mathbf{Q}Gf_a$ is noncommutative, and $\dim_{\mathbf{Q}} \mathbf{Q}Gf_a \geq 4$ for every $a \in C_2^2$. Since $\dim_{\mathbf{Q}} \mathbf{Q}G = 32$, we therefore obtain that $\mathbf{Q}G = \mathbf{Q}Ge \times \prod_{a \in C_2^2} \mathbf{Q}Gf_a$, $\mathbf{Q}Ge$ is a direct sum of fields, and any $\mathbf{Q}Gf_a$ has dimension 4 over $\mathbf{Q}$. So each $\mathbf{Q}Gf_a$ is isomorphic to either $\mathbf{H}(\mathbf{Q})$ or $M_2(\mathbf{Q})$. Hence G is admissible.

(b)–(e) Each of these groups is a homomorphic image of W_2 and thus is admissible by Lemma 7.

(f) Let $G = G_{2^{2n}}^1$. Write $\varphi : G' \to G$ for the monomorphism given by $\varphi(t_{12}^{a_2} t_{13}^{a_3} \cdots t_{1n}^{a_n}) = x_2^{a_2} x_2^{a_3} \cdots x_n^{a_n}$ ($a_i \in C_2$). The set $\mathscr{H}$ of hyperplanes of G' (considered as a vector space over C_2) has exactly $2^{n-1} - 1$ elements. For each $S \in \mathscr{H}$ fix a basis $\{y_1^S, y_2^S, \ldots, y_{n-2}^S\}$. For every $S \in \mathscr{H}$ and every $a = (a_1, a_2, \ldots, a_{n-1}) \in C_2^{n-1}$ let

$$f_S^a = \frac{1}{2^{n-1}}\left(1 + (-1)^{a_1} x_1^2\right) \prod_{i=2}^{n-1} \left(1 + (-1)^{a_i} \varphi\left(y_i^S\right)\right) \hat{S}\left(1 - \widehat{G'}\right).$$

Since $\varphi(y_i^S)\hat{S}$ is central and $(\varphi(y_i^S)\hat{S})^2 = \hat{S}$, it follows easily that each f_S^a is a nonzero central idempotent. One can now verify that

$$\left\{f_S^a | S \in \mathscr{H}, a \in C_2^{n-1}\right\}$$

is a set of $2^{n-2}(2^{n-1} - 1)$ orthogonal nonzero central idempotents of $\mathbf{Q}G$. Since $\dim_{\mathbf{Q}} \mathbf{Q}Gf_S^a \geq 4$ for every $S \in \mathscr{H}$, $a \in C_2^{n-1}$ [3, Lemma 1.2], and because $\dim_{\mathbf{Q}} \mathbf{Q}G\widehat{G'} = 2^{n+1}$ and $\dim_{\mathbf{Q}} \mathbf{Q}G = 2^{2n}$, we obtain that

$$\begin{aligned} 2^{2n} &= 2^{n+1} + 4(2^{n-1})(2^{n-1} - 1) \\ &\leq \dim_{\mathbf{Q}} \mathbf{Q}G\widehat{G'} + \sum_{S \in \mathscr{H}, a \in C_2^{n-1}} \dim_{\mathbf{Q}} \mathbf{Q}Gf_S^a \leq 2^{2n}. \end{aligned}$$

Thus, $\dim_{\mathbf{Q}} \mathbf{Q}Gf_S^a = 4$, and therefore $\mathbf{Q}Gf_S^a$ is isomorphic to either $\mathbf{H}(\mathbf{Q})$ or $M_2(\mathbf{Q})$, for all $S \in \mathscr{H}$ and $a \in C_2^{n-1}$. Since $\mathbf{Q}G = \mathbf{Q}G\widehat{G'} \times \prod_{S \in \mathscr{H}, a \in C_2^{n-1}} \mathbf{Q}Gf_S^a$ it follows that G is admissible.

(g) follows by a similar argument.

(h) is a homomorphic image of (f) and (i) and (j) are homomorphic images of (g). ∎

Because of Lemma 8, to prove (1) $\Rightarrow$ (2) we have to show the following two statements:

(A) Every indecomposable nilpotent admissible finite group G is isomorphic to one of the 10 groups listed in the condition (2) of Theorem 6.

(B) Any two different groups listed in the condition (2) of Theorem 6 are not isomorphic.

Proof of (B). Comparing the orders of the groups G listed, and also comparing the ranks of the groups $G/Z(G)$, it is sufficient to show that: (1) $W_2/\langle x_1^2\rangle \not\cong W_2/\langle x_1^2 t_{12}\rangle$, (2) $G^1_{2^{2n}} \not\cong G^2_{2^{2n}}$, and (3) $G^1_{2^{2n-1}}$, $G^2_{2^{2n-1}}$, and $G^3_{2^{2n-1}}$ are pairwise nonisomorphic.

(1) This follows from the fact that $W_2/\langle x_1^2\rangle$ has a noncentral element of order 2 while $W_2/\langle x_1^2 t_{12}\rangle$ does not.

(2) Clearly x_2 is a noncentral element of order 2 in $G^1_{2^{2n}}$. However, $G^2_{2^{2n}}$ does not have any element satisfying these conditions. Indeed, any noncentral element $x \in G^2_{2^{2n}}$ is of the form $x = z x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ for some nonzero $a = (a_1, a_2, \dots, a_n) \in C_2^n$ and $z \in Z(G^2_{2^{2n}})$. If $a_1 = 0$ then $x^2 = t_{12}^{a_2} \cdots t_{1n}^{a_n} \neq 1$. On the other hand, if $a_1 = 1$, then $x^2 = x_1^2 \neq 1$.

(3) By $C_G(x)$ we denote the centralizer of x in G. Note that $G^1_{2^{2n-1}}$ has a noncentral element $x = x_2$ such that $x^2 = 1$ and $\langle x, Z(G)\rangle \neq C_G(x) \neq G$. However, neither $G^2_{2^{2n-1}}$ nor $G^3_{2^{2n-1}}$ contains such an element. Finally, note that $G^2_{2^{2n-1}}$ has an element $x = x_1$ such that $\langle x, Z(G)\rangle = C_G(x)$ and $x^2 = 1$. But $G^3_{2^{2n-1}}$ does not have such an element. This finishes the proof of (B). ∎

To prove (A) we need to do more work

LEMMA 9. *Let G be a nilpotent admissible finite group such that $G = \langle x_1, \dots, x_n, Z(G)\rangle$. If for a given $i = 1, \dots, n$, $\langle [x_i, x_j] \| j \neq i\rangle \neq G'$, then $x_i^2 \in \langle [x_i, x_j] \| j \neq i\rangle$.*

Proof. Clearly, for any given i, the image of x_i in $H = G/\langle [x_i, x_j] \| j \neq i\rangle$ is central. By Lemma 7, H is admissible. Hence the result follows from Lemma 4. ∎

For a finitely generated group G we denote by $r(G)$ the smallest integer $r(G) \geq 0$ such that is G generated by $r(G)$ elements.

LEMMA 10. *If G is a nonabelian nilpotent admissible finite group, then G is a homomorphic image of some W_n and*

$$r(G) = \min\{m \mid G \text{ is a homomorphic image of } W_m\}.$$

If, furthermore, G is indecomposable and $G/Z(G) = \langle x_1 Z(G), x_2 Z(G), \dots, x_n Z(G)\rangle$ then $G = \langle x_1, x_2, \dots, x_n\rangle$ and thus $r(G) = r(G/Z(G))$.

Proof. Let $x_1, x_2, \ldots, x_n$ be a set of generators of G. By Lemma 4, $x_i^4 = 1$ and $x_i^2 \in Z(G)$ for all i. Furthermore, since $G/Z(G)$ is abelian, $G' \subseteq Z(G)$ and hence $[x_i, x_j] \in Z(G)$ for all $i \neq j$. Therefore, G is a quotient of W_n and it follows that $r(G) = \min\{n | G$ is a homomorphic image of $W_m\}$.

Set $n = r(G/Z(G))$. Let $x_1, \ldots, x_n \in G$ such that $G = \langle x_1, \ldots, x_n, Z(G) \rangle$. Let $H = \langle x_1, \ldots, x_n \rangle$. Since $Z(G)$ is completely reducible, there exists $K \leq Z(G)$ such that $Z(G) = (Z(G) \cap H) \times K$. Therefore $G = H \times K$. So if G is also indecomposable, then $G = \langle x_1, \ldots, x_n \rangle$. Thus, $r(G) = n$. ∎

LEMMA 11. *If a nilpotent finite group G as four elements x_1, x_2, x_3, x_4 such that $[x_1, x_2] \neq 1, [x_3, x_4] \neq 1$, and $[x_i, x_j] = 1$ for every $1 \leq i \leq 2 < j \leq 4$ then G is not admissible.*

Proof. Assume that G is admissible. By Lemma 4, $Z(G)$ and $G/Z(G)$ have exponent 2. So, because of Lemma 7, we may assume that $G = \langle x_1, x_2, x_3, x_4 \rangle$ and $Z(G) = \langle [x_1, x_2] \rangle = \langle [x_3, x_4] \rangle \simeq C_2$. It is not difficult to see that $G/Z(G) \simeq C_2^4$ and $G' \simeq C_2$, but this contradicts [9, Lemma 1.4]. ∎

In the remainder we often reason on a set of elements $x_1, x_2, \ldots, x_n$ of an admissible group G such that $x_1 Z(G), x_2 Z(G), \ldots, x_n Z(G)$ is a basis for $G/Z(G)$ as a vector space over C_2. When we say, for instance, "replacing x_2 by $x_2 x_3$" it is meant that the set $x_1, x_2, \ldots, x_n$ is changed into the set $x_1, x_2\, x_3, x_3, \ldots, x_n$; we denote then again the latter set by $x_1, x_2, \ldots, x_n$. By interchanging x_2 and x_3" is meant that x_2 becomes x_3 and x_3 becomes x_2.

LEMMA 12. *If G is a nilpotent admissible finite group such that $r(G/Z(G)) = 3$, then $r(G') = 2$.*

Proof. By Lemma 8, we may assume that G is indecomposable. Hence by Lemma 10, $G = \langle x_1, x_2, x_3 \rangle$, $Z(G) = \langle t_{i,j} x_k^2 | 1 \leq i < j \leq 3, 1 \leq k \leq 3 \rangle$ and $G' = \langle t_{i,j} | 1 \leq i < j \leq 3 \rangle$, where $t_{ij} = [x_i, x_j] (1 \leq i < j \leq 3)$. By [9, Lemma 1.4], $2 \leq r(G') \leq 3$

Assume $r(G') = 3$, that is t_{12}, t_{13}, t_{23} are linearly independent. If $x_1^2 = x_2^2 = x_3^2 = 1$, then $G_1 = G/\langle t_{12} t_{13}, t_{12} t_{23} \rangle$ is admissible and the image of t_{12}, t_{13}, and t_{23} in G_1 are equal. This implies that the image y of $x_1 x_2 x_3$ in G_1 is a central element and $y^2 \neq 1$. This yields to a contradiction with Lemma 4. Therefore we may assume that $x_1^2 \neq 1$.

By Lemma 9, $x_1^2 \in \langle t_{12}, t_{13} \rangle$, $x_2^2 \in \langle t_{12}, t_{23} \rangle$, and $x_3^2 \in \langle t_{13}, t_{23} \rangle$. We claim that we may assume that $x_1^2 = t_{12}$. Indeed, if $x_1^2 = t_{13}$ then by interchanging x_2 and x_3 we obtain that $x_1^2 = t_{12}$. If $x_1^2 = t_{12} t_{13}$, by replacing x_2 by $x_2 x_3$ we obtain $x_1^2 = t_{12}$, hence proving the claim. By

Lemma 9, since $G = \langle x_1 x_3, x_2, x_3 \rangle$, $t_{13} t_{12} x_3^2 = t_{13} x_1^2 x_3^2 = (x_1 x_3)^2 \in \langle [x_1 x_3, x_2], [x_1 x_3, x_3] \rangle = \langle t_{12} t_{23}, t_{13} \rangle$. Therefore $t_{12} x_3^2 \in \langle t_{12} t_{23}, t_{13} \rangle$ and hence $x_3^2 \in t_{12} \langle t_{12} t_{23}, t_{13} \rangle \cap \langle t_{13}, t_{23} \rangle = \{t_{23}, t_{13} t_{23}\}$. But actually we may assume that $x_3^2 = t_{23}$ by replacing, if necessary, x_3 by $x_1 x_3$. On the other hand, by Lemma 9, since $G = \langle x_1 x_2, x_2, x_3 \rangle$, $x_2^2 = t_{12} x_1^2 x_2^2 = (x_1 x_2)^2 \in \langle [x_1 x_2, x_2], [x_1 x_2, x_3] \rangle \cap \langle t_{12}, t_{23} \rangle = \langle t_{12}, t_{13} t_{23} \rangle \cap \langle t_{12}, t_{23} \rangle = \langle t_{12} \rangle$. Similarly, since $G = \langle x_1, x_2, x_2 x_3 \rangle$, $x_2^2 = t_{23} x_2^2 x_3^2 = (x_2 x_3)^2 \in \langle [x_1, x_2 x_3], [x_2, x_2 x_3] \rangle \cap \langle t_{12}, t_{23} \rangle = \langle t_{12} t_{13}, t_{23} \rangle \cap \langle t_{12}, t_{23} \rangle = \langle t_{23} \rangle$. Thus $x_2^2 \in \langle t_{12} \rangle \cap \langle t_{23} \rangle = \{1\}$. Then taking $y_1 = x_1 x_2, y_2 = x_2$, and $y_3 = x_2 x_3$, one has that $G = \langle y_1, y_2, y_3 \rangle$ and $y_1^2 = y_2^2 = y_3^2 = 1$. But we have already proved that this cannot happen. ∎

LEMMA 13. *If G is a nilpotent admissible finite group such that $r(G/Z(G)) \geq 3$ then there exists three elements $x_1, x_2, x_3 \in G$ such that $[x_2, x_3] = 1$ and $[x_1, x_2]$ and $[x_1, x_3]$ are linearly independent.*

Proof. Let $n = r(G/Z(G))$ and $G = \langle x_1, \dots, x_n, Z(G) \rangle$. Set $t_{ij} = [x_i, x_j]$, $i \neq j$.

If $n = 3$, then by Lemma 12 we may assume (interchanging the x_i's if necessary) that t_{12} and t_{13} are linearly independent and $t_{23} \in \langle t_{12}, t_{13} \rangle$. The statement now follows by considering four cases. For example, if $t_{23} = t_{12} t_{13}$ then we replace x_1, x_2, x_3 by $x_1, x_1 x_3, x_2 x_3$ respectively.

Assume now that $n \geq 4$. Clearly, we may assume $t_{12} \neq 1$. Let $H = \langle t_{ij} | 1 \leq i \leq 2 \leq j \leq n \rangle$. If $r(H) \geq 2$ then we may assume t_{12}, t_{13} are linearly independent and may find the three searched elements in $\langle x_1, x_2, x_3 \rangle$. Otherwise, there exist $3 \leq i < j \leq n$, such that $t_{ij} \notin \langle t_{12} \rangle$ [9, Lemma 1.4]. We may assume $i = 3$ and $j = 4$. By Lemma 11 there exists $1 \leq i \leq 2 < j \leq 4$ such that $t_{ij} \neq 1$ and hence $t_{ij} = t_{12}$. Then the result follows by applying Lemma 12 on the group $\langle x_i, x_3, x_4 \rangle$. ∎

LEMMA 14. *Let G be a nilpotent admissible finite group such that $r(G/Z(G)) \geq 3$. Then there is a subgroup H of G such that $r(H/Z(H)) = r(G/Z(G)) - 1$.*

Proof. Let $n = r(G)$. We argue by induction on n. The result is trivial for $n = 3$.

Assume now that $n \geq 4$ and the result holds for all nilpotent admissible finite groups S with $3 \leq r(S) < n$. Let H be a subgroup of G maximal for the condition

$$r(H/Z(H)) = \max\{r(K/Z(K)) | K \text{ a subgroup of } G, \\ Z(G) \subset K, r(K/Z(K)) \neq n\}.$$

By Lemma 13, $k = r(H/Z(H)) \geq 2$. Let $x_1, x_2, \dots, x_k \in H$ be such that $H = \langle x_1, \dots, x_k, Z(G) \rangle$. Considering $G/Z(G)$ as a vector space over C_2

it is easy to see that there exist $x_{k+1}, \dots, x_n \in G$ such that $G = \langle x_1, \dots, x_n, Z(G) \rangle$. Assume $k \leq n-2$. If $k < i \leq n$ and $K_i = \langle H, x_i \rangle$ then $k \leq r(K_i/Z(K_i)) \leq k+1 < n$. The maximality of H yields that $r(K_i/Z(K_i)) = k$. Therefore, there exists an $h_i \in H$ such that $y_i = h_i x_i \in Z(K_i)$. Consequently $G = \langle x_1, \dots, x_k, y_{k+1}, \dots, y_n, Z(G) \rangle$ and $[x_i, y_j] = 1$ for all $1 \leq i \leq k < j \leq n$. However, this is impossible because of Lemma 11. Thus $k = n-1$. ∎

We need one more essential proposition before being able to prove Theorem 6.

PROPOSITION 15. *Let G be a nilpotent indecomposable nonabelian admissible finite group such that $n = r(G) \geq 3$. Then there exist $x_1, x_2, \dots, x_n$ such that $G = \langle x_1, x_2, \dots, x_n \rangle$, $[x_i, x_j] = 1$ for all $2 \leq i < j \leq n$, and $[x_1, x_2], \dots, [x_1, x_n]$ are linearly independent.*

Proof. Note that, by Lemma 10, G is generated by n noncentral elements, $x_1, x_2, \dots, x_n$. Again set $t_{ij} = [x_i, x_j]$, $i \neq j$. We argue by induction on n. The case $n = 3$ follows from Lemma 10 and Lemma 13.

Assume $n = 4$. By Lemma 13 there are $x_1, x_2, x_3 \in G$ such that t_{12}, t_{13} are linearly independent and $t_{23} = 1$. By considering $G/Z(G)$ as a vector space over C_2 one obtains an $x_4 \in G$ such that $x_1 Z(G), x_2 Z(G), x_3 Z(G), x_4 Z(G)$ are linearly independent in $G/Z(G)$ and $G = \langle x_1, x_2, x_3, x_4 \rangle$ by Lemma 10.

Let $H = \langle x_1, x_2, x_4 \rangle$. By Lemma 12, $r(H') \leq 2$. Since $t_{12} \neq 1$, one has six cases:

1. $t_{24} = 1$
2. $t_{24} = t_{14}$
3. $t_{14} = 1$
4. $t_{24} = t_{12}$
5. $t_{24} = t_{12} t_{14}$
6. $t_{14} = t_{12}$.

In Case 4 (respectively, Case 5), replacing x_4 by $x_1 x_4$ we go to Case 1 (respectively, Case 2). In Case 6, replacing x_4 by $x_2 x_4$ we go to Case 3. Therefore we only have to consider Cases 1, 2, and 3.

Similarly by considering $H = \langle x_1, x_3, x_4 \rangle$ one has the following six cases:

1. $t_{34} = 1$
2. $t_{34} = t_{14}$
3. $t_{14} = 1$
4. $t_{34} = t_{13}$
5. $t_{34} = t_{13} t_{14}$
6. $t_{14} = t_{13}$.

So we have 18 cases by combining the first three cases from the first set with the six cases from the second set. We are going to call case $i.j$ ($i = 1, 2, 3$; $j = 1, \ldots, 6$) the combination of case "i" from the first set and case "j" from the second set. We start with some easy reductions.

Case 3.6. Is impossible because $t_{13} \neq 1$.

Cases 2.1, 3.1, *and* 3.2. First note that Cases 3.1 and 3.2 are the same case. Interchanging x_2 and x_3; Cases 2.1 and 3.1 reduce to Cases 1.2 and 1.3 respectively.

Case 2.2. By replacing x_3 by $x_2 x_3$ this reduces to Case 2.1.

Case 1.6. This reduces to Case 1.3, by replacing x_4 by $x_3 x_4$.

Cases 2.4, 3.4, *and* 3.5. The first two reduce to case 1.5 and 1.3 respectively by interchanging x_2 and x_3 and replacing x_4 by $x_1 x_4$. The third one coincides with Case 3.4.

Now we show that from the remaining cases the only possible one is 1.1.

Case 1.2. Let

$$H = \begin{cases} \langle t_{12} t_{13} \rangle & \text{if } t_{14} \in \langle t_{12}, t_{13} \rangle \\ \langle t_{12} t_{13}, t_{12} t_{14} \rangle & \text{if } t_{14} \notin \langle t_{12}, t_{13} \rangle \end{cases}$$

and $K = G/H$. Then $r(K/Z(K)) = 4$ and $r(K') = 1$, contradicting Lemma 13, and this case is impossible.

Cases 1.3 *and* 2.3. These are the same case. Since x_4 is not central we obtain $t_{34} \neq 1$. Let

$$H = \begin{cases} \langle t_{12} t_{13} \rangle & \text{if } t_{34} = t_{12} \text{ or } t_{34} = t_{13} \\ \langle t_{13} \rangle & \text{if } t_{34} = t_{12} t_{13} \\ \langle t_{12} t_{13}, t_{12} t_{34} \rangle & \text{if } t_{34} \notin \langle t_{12}, t_{13} \rangle \end{cases}$$

and $K = G/H$. Again it follows that $r(K/Z(K)) = 4$ and $r(K') = 1$ and hence this case is excluded.

Case 1.4. Also this case is impossible. For this we argue as in the previous case by taking

$$H = \begin{cases} \langle t_{12} t_{13} \rangle & \text{if } t_{14} \in \langle t_{12}, t_{13} \rangle \\ \langle t_{12} t_{13}, t_{12} t_{14} \rangle & \text{if } t_{14} \notin \langle t_{12}, t_{13} \rangle. \end{cases}$$

Case 1.5. Since Case 1.3 is excluded we obtain $t_{14} \neq 1$. Further, since Case 1.4 is excluded we also have $t_{14} \neq t_{13}$. Again it follows that this case is excluded by arguing as in the previous cases with

$$H = \begin{cases} \langle t_{12}t_{13} \rangle & \text{if } t_{14} = t_{12} \\ \langle t_{13} \rangle & \text{if } t_{14} = t_{12}t_{13} \\ \langle t_{12}t_{13}, t_{14} \rangle & \text{if } t_{14} \notin \langle t_{12}, t_{13} \rangle. \end{cases}$$

Case 2.6. To prove this case is impossible. We argue as in the previous cases by considering

$$H = \begin{cases} \langle t_{12} \rangle & \text{if } t_{34} \in \langle t_{12}, t_{13} \rangle \\ \langle t_{12}, t_{34} \rangle & \text{if } t_{34} \notin \langle t_{12}, t_{13} \rangle. \end{cases}$$

Case 2.5. Since Cases 1.3 and 2.6 are excluded, it follows that $t_{14} \neq 1$ and $t_{14} \neq t_{13}$. Considering $H = \langle t_{13}, t_{12}t_{14} \rangle$ we argue as before to show that this case is excluded.

Case 3.3. First note that because Cases 3.1 and 3.4 are excluded, we obtain $t_{34} \neq 1$ and $t_{34} \neq t_{13}$. Next we show that one may assume that $t_{24} \notin \langle t_{12}, t_{13} \rangle$. If $t_{24} = 1$ then we are in Case 1.3. If $t_{24} = t_{12}$ then replacing x_4 by x_1x_4 again we get Case 1.3. If $t_{24} = t_{13}$ consider $K = G/\langle t_{13} \rangle$. Then the images of the x_i's in K satisfy the conditions of Lemma 11, yielding a contradiction. Finally, if $t_{24} = t_{12}t_{13}$ then by replacing x_4 by x_1x_4 one goes to the case where $t_{24} = t_{13}$ and $t_{14} = 1$ which has been already excluded.

By symmetry one may assume that $t_{34} \notin \langle t_{12}, t_{13} \rangle$.

On the other hand, if $t_{24} = t_{34}$ then by replacing x_2 by x_2x_3 one may assume that $t_{24} = 1$ and again we are in Case 1.3. Thus one may assume that $t_{23} \neq t_{34}$. Take now $K = G/\langle t_{34} \rangle$. It is not difficult to see by using the assumptions made that $r(K/Z(K)) = 4$ and K is thus of type 3.1 which already has been excluded.

Now we deal with the only remaining case.

Case 1.1. That is, there are $x_1, x_2, x_3, x_4 \in G$, such that $G = \langle x_1, x_2, x_3, x_4 \rangle$ and $t_{ij} = 1$ for all $2 \leq i < j \leq 4$. To finish the proof of the proposition for $n = 4$ it only remains to prove that t_{12}, t_{13}, t_{14} are linearly independent. But this is clear as $t_{12}^{a_2}t_{13}^{a_3}t_{14}^{a_4} = 1$ $(a_2, a_3, a_4 \in C_2)$ implies $x_2^{a_2}x_3^{a_3}x_4^{a_4}$ is central and hence $a_2 = a_3 = a_4 = 0$.

Assume now that $n > 4$ and the result holds for all nilpotent admissible finite groups H with $3 \leq r(H/Z(H)) < n$. By Lemma 14, G has a subgroup H such that $r(H/Z(H)) = n - 1$. By the induction hypothesis there are $x_1, \ldots, x_{n-1}$ such that $H = \langle x_1, \ldots, x_{n-1}, Z(H) \rangle$, and $t_{ij} = 1$ for all $2 \leq i \leq n-1$ and $t_{12}, \ldots, t_{1(n-1)}$ are linearly independent. In particular, $r(G') \geq n-2$. Then by Lemma 10, there exists an $x_n \in G$ such that $G = \langle x_1, \dots, x_{n-1}, x_n \rangle$.

First we show that $r(G') \neq n-2$. Suppose the contrary. Then $G' = \langle t_{12}, \dots, t_{1(n-1)} \rangle$. Write $t_{1n} = t_{12}^{a_2} \cdots t_{1(n-1)}^{a_{n-1}}$. Replacing x_n by $x_2^{a_2} \cdots x_{n-1}^{a_{n-1}} x_n$, we may assume that $t_{1n} = 1$. We claim that $t_{in} \in \langle t_{1i} \rangle$ for any $1 < i < n$. If not, then we consider $S = G/\langle t_{1i} \rangle$. We are going to prove that $r(S/Z(S)) = n$. For simplicity we take $i = 2$ and again we denote by x_i and t_{ij} the images of x_i and t_{ij} in S. Note that $t_{13}, \dots, t_{1(n-1)}$ are linearly independent and $t_{2n} \neq 1$ (in S). Suppose $y = x_1^{a_1} \cdots x_n^{a_n} \in Z(G)$ with $a_i \in C_2$, then $1 = [x_2, y] = t_{2n}^{a_n}$ and hence $a_n = 0$. Moreover, $1 = [x_1, y] = t_{13}^{a_3} \cdots t_{1(n-1)}^{a_{n-1}}$ and hence $a_3 = \cdots = a_{n-1} = 0$. Furthermore, $1 = [x_3, y] = t_{13}^{a_1}$ and therefore $a_1 = 0$. Finally, $1 = [x_n, y] = t_{2n}^{a_2}$ and hence $a_2 = 0$. So, we have indeed shown that $r(S/Z(S)) = n$. Since $r(S') = n-3$, this contradicts with the previous paragraph. Hence the claim $t_{in} \in \langle t_{1i} \rangle$ follows. Thus $t_{1n} = 1$ and $t_{in} \in \langle t_{1i} \rangle$ for all $1 < i < n$. Note that since x_n is not central, $t_{in} \neq 1$ for some $2 \leq i \leq n$. Further, $t_{in} \neq t_{1n}$ for some $2 \leq i < n$, since $x_1 x_n$ is not central. Therefore we may assume (by reorganizing if needed) $t_{3n} = t_{13}$ and $t_{2n} = 1$. Let $S = G/\langle t_{12} t_{13} \rangle$ and keep the notation of the x_i's and t_{ij}'s. Then $t_{13}, \dots, t_{1(n-1)}$ are linearly independent in S, $t_{12} = t_{13} = t_{3n}$, and $r(S') = n-3$. As before we derive a contradiction by proving that $r(S/Z(S)) = n$. Let $y = x_1^{a_1} \cdots x_n^{a_n} \in Z(G)$ with $a_i \in C_2$, then $1 = [x_2, y] = t_{12}^{a_1}$ and hence $a_1 = 0$. Moreover, $1 = [x_3, y] = t_{3n}^{a_n}$ and therefore $a_n = 0$. Furthermore, $1 = [x_1, y] = t_{13}^{a_2 + a_3} t_{14}^{a_4} \cdots t_{1(n-1)}^{a_{n-1}}$ and hence $a_4 = \cdots = a_{n-1} = 0$ and $a_2 = a_3$. Finally, $1 = [x_n, y] = t_{3n}^{a_3}$ and thus $a_3 = a_2 = 0$. So we have shown that $r(G') \geq n-1$.

Next we show that $r(G') = n-1$. If $t_{1n} \notin \langle t_{12}, \dots, t_{1(n-1)} \rangle$ and $1 < i < n$, then $r(\langle x_1, x_i, x_n \rangle') \leq 2$ (by Lemma 12) and hence $t_{in} \in \langle t_{1i}, t_{1n} \rangle$. Therefore $G' = \langle t_{12}, \dots, t_{1n} \rangle$. Otherwise, there exists an $1 < i < n$ such that $t_{12}, \dots, t_{1(n-1)}, t_{in}$ are linearly independent. If $1 < j < n$ and $i \neq j$, then by the case $n = 4$, $r(\langle x_1, x_i, x_j, x_n \rangle') \leq 3$ and hence $t_{1n}, t_{j,n} \in \langle t_{1i}, t_{1j}, t_{in} \rangle$. Thus $G' = \langle t_{12}, \dots, t_{1(n-1)}, t_{in} \rangle$.

Therefore, we already know that for every nonabelian nilpotent admissible finite group G, $r(G') = r(G/Z(G)) - 1$.

Let $1 < i < n$. We are going to prove that $t_{in} \in \langle t_{1i} \rangle$. For simplicity take $i = 2$. If not set $S = G/\langle t_{12} \rangle$. Clearly $r(S') = n-2$. We will show that $r(S/Z(S)) = n$ which contradicts the previous paragraph. Again we will abuse notation by keeping the notation x_i and t_{ij} for the homomorphic images in S of the respective elements. Let $y = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in Z(S)(a_1, a_2, \dots, a_n \in C_2)$. Then $[y, x_2] = t_{2n}^{a_n} = 1$ and $t_{2n} \neq 1$. Thus $a_n = 0$. Moreover, $[y, x_3] = t_{13}^{a_1}$ and hence $a_1 = 0$. So $[y, x_1] = t_{13}^{a_3} \cdots t_{1(n-1)}^{a_{(n-1)}} = 1$ and since $t_{13}, \dots, t_{1(n-1)}$ are linearly independent in S, we obtain that $a_j = 0$ for $3 \leq j \leq n-1$. Finally, $[y, x_n] = t_{2n}^{a_2} = 1$ an the assumption implies that $a_2 = 0$.

By considering the group $S = G/\langle t_{1i}t_{1j}\rangle$, $1 < i, j < n$, $i \neq j$, and arguing as before, we can also exclude the possibility $t_{1n} = 1$ and $t_{1j} = t_{nj}$. Thus, either $t_{in} = 1$ for all $1 < i < n$ or $t_{in} = t_{1i}$ for all $1 < i < n$. The second case reduces to the first one by changing x_n by x_1x_n. So this shows the result. ∎

Now we are ready to finish the proof of Theorem 6 by proving the above mentioned statement (A).

Proof of (A). Let G be an indecomposable nonabelian nilpotent admissible finite group. We have to prove that G is isomorphic to one of the groups listed in Theorem 6(2). Let $n = r(G)$.

Assume $n = 2$. By Lemma 10, G is a homomorphic image of W_2. So we have to check only that any nonabelian homomorphic image of W_2 is isomorphic to one of the groups in (a–e) of Theorem 6(2). Let H be a normal subgroup of W_2 such that $G = W_2/H$ is nonabelian. Clearly $H \leq Z(W_2)$ and $t_{12} \notin H$. The statement is trivial if H is trivial or $|H| = 4$. Therefore we may assume $H = \langle a\rangle$ with $a \in Z(G) - \langle t_{12}\rangle$. Thus $a = y^2t_{12}^k$ for some $y \in G - Z(G)$ and $k \in C_2$. Without loss of generality we may assume that $y = x_1$. Thus, if $k = 0$, then $G \simeq W_2/\langle x_1^2\rangle$ and, if $k = 1$, then $G \simeq W_2/\langle x_1^2t_{12}\rangle$.

Now suppose that $n \geq 3$. By Proposition 15, there are $x_1, \dots, x_n$ such that $G = \langle x_1, \dots, x_n\rangle$, $t_{ij} = 1$ for all $2 \leq i < j \leq n$, and $t_{12}, t_{13}, \dots, t_{1n}$ are linearly independent. By Lemma 9, $x_i^2 \in \langle t_{1i}\rangle$ for all $2 \leq i \leq n$, and thus since G is a homomorphic image of W_n, $Z(G) = \langle t_{12}, \dots, t_{1n}, x_1^2\rangle$.

We claim that either $x_i^2 = 1$ for all $2 \leq i \leq n$ or $x_i^2 = t_{1i}$ for all $2 \leq i \leq n$. Assume the contrary. By reorganizing the x_i's, if needed, we may assume that $x_2^2 = 1$ and $x_3^2 = t_{13}$. Then $G = \langle x_1, x_2, x_2x_3, x_4, \dots, x_n\rangle$ and $(x_2x_3)^2 = t_{13} \notin \langle [x_1, x_2x_3]\rangle$. This is in contradiction with Lemma 9 and the claim follows.

So it is sufficient to deal with the following five cases.

1. $x_i^2 = 1$ for all $2 \leq i \leq n$ and $x_1^2 \notin G'$.
2. $x_i^2 = 1$ for all $2 \leq i \leq n$ and $x_1^2 \in G'$.
3. $x_i^2 = t_{1i}$ for all $2 \leq i \leq n$ and $x_1^2 \notin G'$.
4. $x_i^2 = t_{1i}$ for all $2 \leq i \leq n$ and $x_1^2 = 1$.
5. $x_i^2 = t_{1i}$ for all $2 \leq i \leq n$ and $x_1^2 \in G' - \{1\}$.

Case 1. Since $[x_i, x_j] = 1$ for all $2 \leq i < j \leq n$ and $x_i^2 = 1$ for all $2 \leq i \leq n$, then G is a homomorphic image of $G^1_{2^{2n}}$. Furthermore, $r(Z(G)) = r(G/Z(G)) = n$ and hence $|G| = 2^{2n} = |G^1_{2^{2n}}|$. Thus $G \simeq G^1_{2^{2n}}$.

Case 2. Assume $x_1^2 = t_{12}^{a_2} \cdots t_{1n}^{a_n}$. By replacing x_1 by $x_1x_2^{a_2} \cdots x_n^{a_n}$ one may assume that $x_1^2 = 1$. Then, G is a homomorphic image of $G^1_{2^{2n-1}}$ and both groups have the same order. Thus $G \simeq G^1_{2^{2n-1}}$.

Case 3. Arguing as in Case 1 one proves that in this case $G \simeq G^2_{2^{2n}}$.

Case 4. One proves that in this case $G \simeq G^2_{2^{2n-1}}$.

Case 5. Let $x_1^2 = t_{12}^{a_2} \cdots t_{1n}^{a_n}$. By reorganizing the x_i's if needed one may assume that $a_2 = 1$. Then by changing x_1 by $x_1 x_3^{a_3} \cdots x_n^{a_n}$ one may assume that $x_1^2 = t_{12}$. Then as in previous cases one proves that $G \simeq G^3_{2^{2n-1}}$. ∎

REFERENCES

1. S. A. Amitsur, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* **80** (1955), 361–386.
2. B. Banieqbal, Classification of finite subgroups of 2 × 2 matrices over a division algebra of characteristic zero, *J. Algebra* **119** (1988), 449–512.
3. D. B. Coleman, Finite Groups with Isomorphic Group Algebras, *Trans. Amer. Math. Soc.* **105** (1962), 1–8.
4. Ch. W. Curtis and I. Reiner, "Methods of Representation Theory," Wiley, New York, 1981.
5. E. Jespers, Free normal complements and the unit group of integral group rings, *Proc. Amer. Math. Soc.* **122**, No. 1 (1994), 59–66.
6. E. Jespers and G. Leal, Describing units of integral group ring of some 2-groups, *Comm. Algebra* **19**, No. 6 (1991), 1809–1817.
7. E. Jespers and G. Leal, Generators of large subgroups of the unit group of integral group rings, *Manuscripta Math.* **78** (1993), 303–315.
8. E. Jespers and G. Leal, Degree 1 and 2 representations of nilpotent groups and applications to units of group rings, *Manuscripta Math.* **86** (1995), 479–498.
9. G. Leal and C. Polcino Miles, Isomorphic group (and loop) algebras, *J. Algebra* **155** (1993), 195–210.
10. M. Newman, "Integral Matrices," Academic Press, New York, 1972.
11. D. S. Passman, "Permutation Groups," Benjamin, New York, 1968.
12. S. K. Sehgal, "Topics in Group Rings," Dekker, New York, 1978.
13. S. K. Sehgal, "Units of Integral Group Rings," Longman Scientific, Essex, 1993.